IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANTS:	Boivie et al.	DOCKET: YOR920030398US1 (8728-647)
SERIAL NO.:	10/677,933	GROUP ART UNIT: 2132
FILED:	October 1, 2003	EXAMINER: Almedia, Devin E.
FOR:	**COMPUTING DEVICE THAT SECURELY RUNS AUTHORIZED SOFTWARE**	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

This Appeal is from the Advisory Action dated April 23, 2008 and the Final Office Action mailed on February 8, 2008 (hereinafter, referred to as the "Final Action") finally rejecting Claims 11, 13, 14, 16-19, and 22-28 of the above-identified application. The Appellants commenced this Appeal by a Notice of Appeal and Pre-Appeal Brief Request for Review filed on May 8, 2008 (Notice of Panel Decision from Pre-Appeal Brief Review mailed May 16, 2008), and hereby submit this Appeal Brief in furtherance of the Appeal.

TABLE OF CONTENTS

1. Real Party in Interest

The real party in interest is International Business Machines Corporation, the assignee of the entire right, title, and interest in and to the subject application by virtue of an assignment of record.

2. Related Appeals and Interferences

(None)

3. Status of Claims

Claims 11, 13, 14, 16-19, and 22-28 are pending, stand rejected and are under appeal. The claims are set forth in the attached Appendix. Claims 11, 22 and 23 are the independent claims. Claims 1-10, 12, 15, 20-21 has been canceled.

4. Status of Amendments

No After Final Amendments have been filed.

5. Summary of Claimed Subject Matter

In general, the claimed inventions are directed to systems and methods for ensuring that a processor will execute authorized code.

Claim 11 recites:

A method for ensuring that a processor will execute only authorized code, said method comprising:

reading a certificate including a first public key into a protected memory (see for example, FIG. 7, 701 and page 16, lines 13-14);

validating said certificate with a second public key permanently stored on said processor (see for example, FIG. 7, 702 and page 16, lines 14-15);

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected (see for example, FIG. 7, 703 and page 16, lines 17-18);

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key (see for example, FIG. 7, 704 and page 16, lines 18-19); and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing inline decryption of the copy of said signed authorized code in said protected memory (see for example, FIG. 7, 706 and page 17, lines 2-3) upon verifying said digital signature (see for example, FIG. 7, 705 and page 16, line 20 to page 17, line 1).

Claim 22 recites:

A program storage device readable by machine, tangibly embodying a program of

instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code (see for example, FIG. 2 and page 6, line 18 to page 7, line 6), the program steps comprising:

reading a certificate including a first public key into a protected memory (see for example, FIG. 7, 701 and page 16, lines 13-14);

validating said certificate with a second public key permanently stored on said processor (see for example, FIG. 7, 702 and page 16, lines 14-15);

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected (see for example, FIG. 7, 703 and page 16, lines 17-18);

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key (see for example, FIG. 7, 704 and page 16, lines 18-19); and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing inline decryption of the copy of said signed authorized code in said protected memory (see for example, FIG. 7, 706 and page 17, lines 2-3) upon verifying said digital signature (see for example, FIG. 7, 705 and page 16, line 20 to page 17, line 1).

Claim 23 recites:

A computing device for securely executing authorized code, said computing device comprising:

a protected memory (see for example, FIG. 2, 216) for storing signed authorized code (see for example, FIG. 1, 101), which contains an original digital signature (see for example, 102, FIG. 1), wherein said protected memory is cryptographically protected; and

a processor (see for example, FIG. 2, 210) in signal communication with said protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in said signed authorized code is original in accordance with a first public key stored in said protected memory (see for example, FIG. 1, 103), said first public key validated by a second public key permanently stored on said processor, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution (see for example, FIG. 1, 104).

6. Grounds of Rejection to be Reviewed on Appeal

A. Claims 11, 13, 14, 16, 18 and 22-26 have been rejected under 35 U.S.C. 102(b) as being unpatentable over Sudia et al. (USPAN 2001/0050990).

B. Claims 17, 19, 27 and 28 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Morgan et al. (USPN 6,185,685).

7. **Argument**

A. **Claim Rejections - 35 U.S.C. §102**

i. Claims 11, 13, 14, 16, 18 and 22-26

For a claim to be anticipated under 35 U.S.C. §102, all elements of the claim must be found in a single prior art reference (see, e.g., Scripps Clinic & Research Found. v. Genentech Inc., 927 F.2d 1565, 1576, 18 U.S.P.Q.2d. 1001, 1010 (Fed. Cir. 1991)). The identical invention must be shown in as complete detail as is contained in the claim. (See MPEP § 2131). The single prior art reference must disclose all of the elements of the claimed invention functioning essentially in the same manner (see, e.g., Shanklin Corp. v. Springfield Photo Mount Corp. 521 F.2d 609 (1st Cir. 1975)).

The anticipation rejections of Claims 11, 13, 14, 16, 18 and 22-26 are legally deficient as a matter of law and fact: Sudia teaches a cryptographic system with a key escrow feature (see Abstract). Sudia does not teach "preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key" as claimed in Claims 11 and 22 nor "a processor… verifying that a digital signature contained in said signed authorized code is original in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor" as claimed in Claim 23. Sudia teaches that a tamper-resistant trusted device that contains an embedded manufacturer's public key, wherein the device accepts input containing new or additional firmware code signed using a manufacturer's signature and verifies the manufacturer's signature using a public signature key of the manufacturer (see paragraph [0248]). Respectfully, the manufacturer's signature of Sudia is not analogous to the claimed first public key. Consider that, Sudia does not teach that the

manufacturer's signature is used to verify a digital signature of the new or additional firmware code, wherein the digital signature is later used to verify a digital signature; according to Sudia *the function of verification is performed in every instance using with the public signature key of the manufacturer* (see for example, paragraphs [0072] and [0249]). Thus, Sudia does not teach a validation of a first public key using the public signature key of the manufacturer, the first key which is then used for verifying digital signatures, essentially as claimed.

Turning now to the manufacture's certificate or update certificate of Sudia; consider that Sudia teaches in paragraph [0249] that a method 1) signs an update certificate containing a public key of a third party firmware, 2) verifies a third party signature (associated with code) using the update certificate, and 3) verifies the update certificate using a manufacturer's public signature key. The claimed invention 1) validates a certificate (associated with a first public key) using a second public key permanently stored in a processor and then 2) verifies authorized code using the first public key. Sudia's update certificate is clearly not analogous to the first public key in that it is not associated with a certificate itself. Further, the upgrade certificate is issued directed by the manufacturer – the update certificate is not verified using the manufacturer's public signature as an initial matter so that it may be later used to verify the third party signature. Indeed Sudia is silent on the steps used in issuing the upgrade certificate. Also note that Sudia's *verification always has at its terminus the manufacturer's public signature key* (see paragraph [0249], second to last sentence) – the update certificate is evidently not a trusted means for verification in and of itself and no branching is performed upon a verification using the update certificate – Sudia requires that *the manufacturer's public signature key* be used for verification prior to any desired function. Sudia does not verify the code using a verified key nor perform a branch operation upon such a verification; Sudia's verification is the exclusive province of the

manufacturer's public signature key.

Therefore, Sudia fails to teach all the limitations of Claims 11, 22 and 23.

Claims 13, 14, 16-19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. Claims 15, 20 and 21 have been cancelled.

Withdrawal of the rejections under 35 U.S.C. §102, is respectfully requested.

B. The Claim Rejections Under 35 U.S.C. §103

i. Claims 17, 19, 27 and 28

Claims 17 and 19 depend from Claim 11. Claims 27 and 28 depend from Claim 23. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims.

Withdrawal of the rejections under 35 U.S.C. §103, is respectfully requested.

C. Conclusion

In view of the foregoing, it is respectfully requested that the Board overrule the rejections of Claims 11, 13, 14, 16-19, and 22-28.

Respectfully Submitted,

Date: July 8, 2008

By: /Nathaniel T. Wallace/
Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Appellants

F. CHAU & ASSOCIATES, LLP
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889

8. CLAIMS APPENDIX

1-10. (Canceled)

11. A method for ensuring that a processor will execute only authorized code, said method comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected;

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key; and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing inline decryption of the copy of said signed authorized code in said protected memory upon verifying said digital signature.

12. (Canceled)

13. A method as recited in claim 11 wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor.

14. A method as recited in claim 11 wherein said protected memory is physically protected.

15. (Canceled)

16. A method as recited in claim 11 wherein the integrity of said authorized code is protected at run time.

17. A method as recited in claim 16 wherein the integrity of said authorized code is protected with symmetric key encryption.

18. A method as recited in claim 11 wherein the privacy of said authorized code is protected at run time.

19. A method as recited in claim 18 wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

20-21. (Canceled)

22. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected;

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key; and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing inline decryption of the copy of said signed authorized code in said protected memory upon verifying said digital signature.

23. A computing device for securely executing authorized code, said computing device comprising:

a protected memory for storing signed authorized code, which contains an original digital signature, wherein said protected memory is cryptographically protected; and

a processor in signal communication with said protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in said signed authorized code is original in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution.

24. A computing device as recited in claim 23 wherein the integrity of the contents of said protected memory is protected by encryption.

25. A computing device as recited in claim 23 wherein said protected memory is physically protected.

26. A computing device as recited in claim 23 wherein at least one of the integrity of said authorized code and the privacy of said authorized code is protected at run time.

27. A computing device as recited in claim 23 wherein the integrity of said signed authorized code is protected at run time with symmetric key encryption.

28. A computing device as recited in claim 23, wherein the privacy of said signed authorized code is protected at run time with symmetric key encryption.

9. EVIDENCE APPENDIX

(None)

10. RELATED PROCEEDINGS APPENDIX

(None)